Department of Veterans Affairs **VA HANDBOOK 6502.1**
Washington, DC 20420 **Transmittal Sheet**
March 25, 2004

PRIVACY VIOLATION TRACKING SYSTEM (PVTS)

1. REASON FOR ISSUE: This handbook establishes Department-wide procedures for the One VA Privacy Violation Tracking System (PVTS), and implements the policies set forth in Department of Veterans Affairs (VA) Directive 6502, Privacy Program.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: In accordance with provisions of VA Directive 6502, Privacy Program, and in order to centralize and monitor the privacy complaint resolution process, the VA Office of Cyber and Information Security (OCIS) Privacy Service has established the PVTS. This handbook describes the responsibilities, requirements, and procedures for this process. The PVTS serves as a central repository of privacy-related complaints and violations. The PVTS provides a Department-wide log of privacy-complaints that are registered by VA personnel, and veterans, their dependents, and beneficiaries under applicable Federal privacy laws and regulations. The complaints are addressed by VA Privacy Officers (PO) in compliance with applicable Federal privacy laws and regulations.

3. RESPONSIBLE OFFICE: Office of Cyber and Information Security (005S), Office of the Assistant Secretary for Information and Technology (005).

4. RELATED DIRECTIVE: VA Directive 6502, Privacy Program.

5. RESCISSIONS: None

CERTIFIED BY:

/s/
Robert N. McFarland
Assistant Secretary for
Information and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Robert N. McFarland
Assistant Secretary for
Information and Technology

Distribution: RPC: 6002

FD

PRIVACY VIOLATION TRACKING SYSTEM

CONTENTS

PRIVACY VIOLATION TRACKING SYSTEM (PVTS)

1. PURPOSE AND SCOPE

a. This handbook provides the procedures and requirements for recording privacy-related complaints and violations in the One VA Privacy Violation Tracking System (PVTS). The PVTS is a component of the Department of Veterans Affairs (VA) Privacy Program, mandated in VA Directive 6502, Privacy Program, and administered by the VA Office of Cyber and Information Security (OCIS) Privacy Service.

b. Federal privacy regulations and guidance provide individuals with a right to complain about the manner in which VA maintains their privacy-protected data, or any other private information, and any observed or perceived lapses in VA's protection of private information. The PVTS provides a VA-wide centralized, auditable database of all privacy complaints and violations.

c. The PVTS documents all potential privacy complaints and violations received or observed by VA Privacy Officers (PO). It also provides statistics to the Privacy Service and VA management. This system supports the "documentation of complaints" requirement in the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, 45 CFR Parts 160 and 164, as published by the Department of Health and Human Services (HHS). In order to achieve consistent privacy practices throughout the Department, this system is for use VA-wide. However, it is not intended to replace existing practices for documenting information requests made under either the Freedom of Information Act (FOIA) or the Privacy Act.

d. This handbook identifies the minimal required elements for the documentation of the complaint registration and resolution process in the PVTS. It also provides the procedures for VA Privacy Service audit of these complaints.

2. RESPONSIBILITIES

a. **Director, Privacy Service.** The Director shall establish the One VA procedure for tracking and auditing VA privacy violations and complaints by:

(1) Assigning, implementing, and managing a Department-wide system to track the complaints and reports of privacy-related violations;

(2) Providing a current user manual explaining the functions and reporting requirements of the Department-wide system, and instructions on the use of the PVTS to POs;

(3) Maintaining audit records and documentation provided by the tracking system;

(4) Reporting to oversight agencies and VA management on privacy violation and complaint resolution within VA, as required;

(5) Providing oversight and guidance for VA compliance with applicable law relating to complaint and privacy-related violations;

(6) Designating the PVTS as the complaint monitoring system, in accordance with the requirements of VA Directive 6502, Privacy Program;

(7) Setting the requirements and access rights for submission of all potential privacy violations to the PVTS; and

(8) Establishing, maintaining, and enforcing the security and privacy requirements of the PVTS and the records that it generates, stores, and transmits.

b. **Director, Business Assurance Service.** The Director shall periodically review the PVTS database of complaints for security violations.

c. **The Inspector General.** This Office will be requested to:

(1) Review and monitor the Privacy Service audits of the PVTS;

(2) Provide assistance and guidance to the Privacy Service in the conduct and design of PVTS audits; and

(3) Provide recommendations on the complaint resolution process.

d. **Under Secretaries, Assistant Secretaries, and Other Key Officials.** These officials shall:

(1) Ensure that POs report all actual or suspected breaches of and complaints regarding privacy to the PVTS, as soon as possible;

(2) Ensure that POs, and other authorized users, record all updates and resolutions of privacy complaints and violations to the PVTS, as soon as possible; and

(3) Provide guidance on the complaint referral process.

e. **Privacy Officers (PO).** POs shall:

(1) Report all potential privacy violations and complaints to the PVTS, as soon as possible;

(2) Update and resolve all privacy violations and complaints, as soon as possible; and

(3) Obtain and maintain their PVTS license and password.

f. **The VA Central Incident Response Capability (VA-CIRC).** The VA-CIRC shall:

(1) Provide the tracking system database in accordance with the security and privacy requirements established by the Privacy Service; and

(2) Train VA-CIRC call center personnel according to the requirements for the PVTS established by the Privacy Service.

3. ESSENTIAL REQUIREMENTS AND PROCEDURES

a. **General Procedures.** POs are responsible for recording all privacy-related complaints and violations, their updates, and resolutions to the PVTS, as soon as possible. The PVTS will generate statistical reports about the number and status of complaint Tickets in accordance with requirements provided by the Privacy Service. The Web-based PVTS enters the complaints into a database that is monitored and audited by the Privacy Service. The PVTS manager maintains the database and provides secure and limited access to it through a system of user licenses and passwords. The PVTS will provide for the referral of complaints and violations through the privacy hierarchy in the appropriate VA organization or facility. The PVTS consists of recording complaints, violations, and their resolution into complaint Tickets, an automatic escalation of delinquent Tickets, and reporting on the statistics of privacy complaints and/or violations.

b. **Recording Complaints and Violations.** A complaint or violation is recorded when it is entered into the PVTS via a Web-based form, hereafter referred to as the Ticket. A description of each menu and instructions for using the Web-based system can be found in the PVTS manual provided by the Privacy Service. The required elements of the recording procedure are:

(1) Entering a complaint or violation into the PVTS by one of two ways:

(a) The PO enters a complaint or violation into the PVTS by opening a Ticket, as soon as possible after the complaint is received or violation is observed; or

(b) The VA-CIRC receives a complaint through its call center (via phone or email) and enters the complaint into the PVTS by opening a Ticket and assigning the Ticket to the appropriate PO. The appropriate PO is then notified of the opened ticket and assumes responsibility for the resolution of the complaint.

(2) The complaint or violation must be categorized by the PO according to the type of sensitive information potentially breached. The PVTS lists the information categories in a menu.

(3) A complete description of the nature of the complaint or violation must be entered into the Ticket.

(4) The complaint or violation must be further defined according to the type of breach of privacy that is alleged. The following types of breaches illustrate the categories that will be specified in the PVTS manual, listed in a PVTS menu, and updated as required:

(a) Safeguard breaches, which include the security of personal information such as breaches in administrative, technical, and physical safeguards;

(b) Collection breaches, which include compilation of personal information that is not authorized, relevant, or necessary, as provided in applicable law;

(c) Disclosure breaches, which include the communication of personal information in any medium without proper authority, or in an improper manner;

(d) Usage breaches, which include sharing, examination, or analysis of personal information that is not required for the official performance of authorized VA duties under applicable law;

(e) Disposal breaches, which include unauthorized deletion or destruction of personal information or improper disposal of properly discarded material; and

(f) Access and amendment complaints, which pertain to complaints of denial of access and amendment rights that are specific to the requirements of the HIPAA Privacy Rule.

c. **Resolution of Complaints and Violations.** The PO must resolve each complaint and violation as soon as possible. The types of corrective actions may include, but are not limited to, education, reprimand, or sanction. The following types of corrective actions are illustrative of the categories that are specified in the PVTS manual and will be updated as required:

(1) **Education**. If the PO or resolving authority (i.e., the privacy hierarchy) determines that the breach occurred because VA personnel were not informed of their responsibilities, or the requirements for the proper use, disclosure, or collection of personal information, the category Education is selected and remedial training is assigned.

(2) **Reprimand**. If the PO or resolving authority determines that VA personnel have engaged in unacceptable actions or inactions resulting in the reported breach, the category Reprimand is selected.

(3) **Sanction**. If the PO or resolving authority determines that VA personnel have engaged in unacceptable actions that warrant personnel sanctions, the category Sanction is selected.

(4) **No Breach**. If the PO or resolving authority determines that the reported complaint or violation is not a breach under provision of law, the category No Violation is selected.

d. **Referral of Complaints and Violations through the Privacy Hierarchy.** If the PVTS call center receives a complaint or violation directly from the complainant then the call center refers the complaint to the appropriate PO. If a PO cannot resolve the complaint or violation then he or she should refer the complaint or violation to the next level of the privacy hierarchy within his or her organization or facility, as soon as possible.

e. **Referral to the Secretary of Health and Human Services**. If the PO or resolving authority determines that VA cannot address all aspects of a complaint that falls within the scope

of the HIPAA Privacy Rule, then the complainant may be referred to the Secretary of Health and Human Services.

4. ESCALATION

a. Typically each Administration and staff office assigns POs in a hierarchy beginning at the facility level, and moving up to regional and headquarters levels. The number of levels will vary with the size of the Administration or staff office. This hierarchy will be observed when following complaints through the PVTS resolution process.

b. If a complaint or violation has not been acted upon, or does not show a change of status in a period of time designated by the Privacy Service, the Ticket will automatically escalate to the next level in the PO hierarchy chain. The next, higher level PO will be automatically notified that he or she is now responsible for resolving the complaint.

c. Complaints or violations that cannot be resolved within the Administrations or staff offices, such as complaints pertaining to cross-organizational procedures, will be escalated to the VA Privacy Service.

5. AUDIT

a. Records of the number, type, resolution, and status of complaints and violations will be maintained in the PVTS. The PVTS will generate statistical analyses of these records according to direction provided by the Privacy Service. Only the Privacy Service will have access to all records and reports. POs will have access to the statistical reports and complaint Tickets that fall under their authority. Information on how to generate reports is provided in the PVTS manual.

b. The Privacy Service will monitor the PVTS database and provide periodic reports of the VA-wide status of privacy-related violations and complaints. The Privacy Service will provide these reports to the VA Chief Information Officer (CIO), each Administration, and to other entities or Federal agencies in compliance with applicable privacy law.

6. REFERENCES

a. Freedom of Information Act (FOIA), 5 U.S.C. 552.

b. Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. 104-191.

c. HIPAA Privacy Rule, 45 CFR Parts 160 and 164.

d. OMB Circular A-130, Management of Federal Information Resources, Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals.

e. OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Systems, February 8, 1996.

f. Privacy Act of 1974, 5 U.S.C. 552a.

g. Privacy Violation Tracking System Manual.

h. VA Directive and Handbook 6210, Automated Information Systems Security.

i. VA Directive 6212, Security of External Electronic Connections.

j. VA Directive 6213, VA Public Key Infrastructure.

k. VA Directive 6214, Information Technology Security Certification and Accreditation Program.

l. VA Handbook 6300.2, Management of the Vital Records Program.

m. VA Handbook 6300.3, Procedures for Implementing the Freedom of Information Act (FOIA).

n. VA Handbook 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act (PA).

o. VA Handbook 6300.5, Procedures for Establishing and Managing Privacy Act Systems of Records.

p. VA Handbook 6300.6, Procedures for Releasing Lists of Veterans' and Dependents' Names and Addresses.

q. VA Handbook 6300.8, Procedures for Shipment of Records to the VA Records Center and Vault in Neosho, Missouri.

r. VA Handbook 6301, Procedures for Handling Electronic Mail Records.

s. VA Handbook 6330, Directives Management Procedures.

t. VA Handbook 6360.1, Procedures for Implementation of the Government Information Locator Service (GILS).

u. VA Directive 6502, Privacy Program.

v. 5 CFR Parts 731, 732, and 736.

w. 38 U.S.C. 5701, Confidential Nature of Claims.

x. 38 U.S.C. 5705, Confidentiality of Medical Assurance Records, 17.500-.511.

y. 38 U.S.C. 7332, Confidentiality of Certain Medical Records, 1.460-.496.

7. DEFINITIONS

a. **Breach of Privacy Rights.** Any access, communication, use, or disposal of personal information that is in noncompliance with applicable Federal privacy law and regulations.

b. **Complaint.** For the purposes of this handbook, the formal registration of any grievance concerning an actual or suspected breach of privacy of personal information under Federal privacy law and regulations.

c. **Complaint Ticket ("Ticket").** The PVTS Web-based form in which each complaint or violation is recorded and tracked.

d. **Privacy Hierarchy.** The organization of each Administration's and staff office's cadre of POs according to increasing responsibilities and authority over privacy-related matters.

e. **PVTS Call Center.** A branch of the VA-CIRC that receives privacy-related complaints by telephone or email, enters these complaints into the PVTS database, and refers each complaint to the appropriate PO.

f. **Resolution Authority.** The PO, within the PO hierarchy, with the authority and responsibility to resolve complaints and violations.

g. **Resolution of Complaint.** The corrective action taken by the PO, or authorized user, in accordance with VA policy, in response to a complaint. Includes "no action necessary" if complaint determined to be unfounded.

h. **Violation.** For the purposes of this handbook, the observance by the PO of any actual or suspected breach of privacy of personal information under Federal privacy law and regulation.